OFFICE OF INFORMATION TECHNOLOGY (OIT)

PROJECT LEADER HELP GUIDE

JANUARY, 2006

HUD.GOV V6.0

TABLE OF CONTENTS

INTRODUCTION

HUD has standards and procedures in place for Information Technology (IT) project planning and system development. Successful projects at HUD all demonstrate a common theme of adherence to these standards and procedures.

The Office of Information Technology (OIT) has identified several key standards and procedures that, if followed, will ensure successful IT projects at HUD.

These standards and procedures cover the operational and development platforms, security, configuration management, the development process itself, as well as IT Capital Planning.

Following the standards and processes below will reduce potential project roadblocks or unnecessary delays. If a developer or Project Leader understands and follows these processes, the end product will be a well-rounded, thoroughly planned project that complies with HUD policies and objectives.

SYSTEM DEVELOPMENT

- Access to the Development Environment
- Configuration Change Management Board (CCMB)
- Configuration Management (CM)
- Data Quality
- HUD Open Integration Guidelines (HOIG)
- HUD Test Center (HTC) and the Software Release Process
- Inventory of Automated Systems (IAS)
- Section 508 Compliance
- Security
    - Major Applications
    - General Support Systems
    - A-130 Reviews
- System Development Methodology (SDM)

IT CAPITAL PLANNING AND INVESTMENT MANAGEMENT

- Enterprise Architecture
- IT Capital Planning
- Software Acquisition Initiative (SA-CMM)

CONTINGENCY PLANNING

- Continuity of Operations Plan (COOP)

HUD ENVIRONMENT

- Contracting
- Offsite Contractor Connectivity
- IT Help at HUD

This Guide is written as a quick-start tool to help the new Project Leader or developer understand how HUD works and how to successfully plan and manage an IT project at HUD. It is structured as a roadmap to help you understand and navigate through key processes and standards.

SYSTEM DEVELOPMENT

The OIT has determined the ability of a Project Leader to understand and/or navigate the following key standards and system development processes will lead to the successful deployment of a project at HUD. Additional key processes and standards important to the development process will be added to future versions of this Guide.

- Access to the Development Environment
- Configuration Change Management Board (CCMB)
- Configuration Management (CM)
- Data Quality
- HUD Open Integration Guidelines (HOIG)
- HUD Test Center (HTC) and the Software Release process
- Inventory of Automated Systems (IAS)
- Section 508 Compliance
- Security
    - Major Applications
    - General Support Systems
    - A-130 Reviews
- System Development Methodology (SDM)

ACCESS TO THE DEVELOPMENT ENVIRONMENT

For a development staff to effectively develop and test a system within the IT environment at HUD, a Project Leader must provide access to the appropriate development resources.

Submit access requests by email to the appropriate HUD staff member for your project and be sure to follow current established procedures. Allow 3-5 working days for access to be granted.

A) WHAT

Obtain access to the HUD development resources/servers the development team requires.

B) WHY

Without proper access, your development team will be unable to develop and test in the HUD environment.

C) WHEN

Request access once the development team has been selected; request again as additional developers are added to the project team.

CONFIGURATION CHANGE MANAGEMENT BOARD (CCMB)

All hardware, software and development projects must use approved HUD infrastructure or development standards. Any new hardware, software or development effort requiring the use of other than currently approved products or processes must be reviewed and approved by the Configuration Change Management Board (CCMB) prior to usage.

HUD established the Configuration Change Management Board (CCMB) as the formal vehicle to make changes to the IT infrastructure and system development platforms, as well as the full suite of development tools. The CCMB makes decisions regarding the implementation of any product or development process that is not a HUD Standard.

If you are developing a project that will require the use of a non-HUD Standard, adhere to the following process:

A) WHAT

Know the approved **HUD Standards** and use them in developing your system. When it is not possible to use a HUD Standard for your project, submit a request to use a non-HUD Standard to the CCMB and obtain approval for usage.

- ✓ Any non-HUD standard product submitted for CCMB approval must comply with HUD Section 508 policies

B) WHY

Your application will not be able to pass release testing **AND** your system will not be released into production without CCMB approval of non-standard components.

C) WHEN

Submit a request to the CCMB as soon as you know usage of a non-HUD Standard is required for your project.

CONFIGURATION MANAGEMENT (CM)

Configuration Management (CM) helps maintain version control over all project artifacts. All HUD systems and SDM documentation must be under CM.

Develop a strong **Configuration Management Plan (CMP)** and ensure you and your development team follow the guidelines closely. HUD policy requires the development of a CMP consistent with HUD CM Procedures using the HUD-approved CM software tool appropriate for the project. HUD-approved CM tools are listed on the **IT Standards** page of **hud.gov**.

A) WHAT

Develop, implement, and maintain a **CMP** for all HUD systems. The scope of your **CMP** should include the required SDM documentation.

B) WHY

A **CMP** is required for all HUD systems.

In addition, Configuration Management (CM) reduces the risk of unauthorized or undocumented changes to the HUD applications and related project documentation your team is developing.

Adhering to good CM practices helps you and your team to maintain version control over the system and supporting documentation.

C) WHEN

A **CMP** is developed early in the project and should provide for the control of hardware, software, and documentation configuration items. Subsequently, the **CMP** is updated during the Define and Design System phases of the SDM lifecycle to define how development artifacts are tracked as well as to allow for any changes made prior to implementation.

DATA QUALITY

The **Total Information Quality Management (TIQM)** initiative focuses on improving the quality of mission-critical information in HUD IT systems. Mission-critical information is information that is considered fundamental for HUD to conduct business, or information key to the Department's accountability and integrity, and information used to support Annual Performance Plans. The TIQM process falls within the purview of the Data Control Board (DCB) and the Enterprise Data Management Group (EDMG).

The TIQM approach is based on accepted industry standards, and incorporates project management and total quality management principles. It is an iterative approach to process and data quality improvement that can be repeated until appropriate measurable quality levels are achieved.

The TIQM environment defines key components and characteristics of information quality, and also establishes quality standards for mission-critical information.

TIQM is a four-stage process: assessment, process improvement, correction, and certification. The OCIO is responsible for the assessment and certification of mission-critical information, whereas Program Area managers and system sponsors are responsible for process improvement and data correction.

A) WHAT

Become familiar with the **HUD Enterprise Data Management Policy** and **HUD TIQM environment**. Data quality should be a basic design element of all HUD system development and maintenance efforts.

B) WHY

The Department must ensure that it's financial and programmatic information have a level of quality that makes the information credible and useful both inside and outside of HUD. Program Area management and system sponsors are accountable for the quality of their information.

C) WHEN

Data quality is a requirement throughout the entire system lifecycle, from design and development to operations, maintenance, and disposition.

HUD OPEN INTEGRATION GUIDELINES (HOIG)

The HUD Open Integration Guidelines (HOIG) is a set of guidelines designed for development teams to facilitate the integration of a system into the HUD network infrastructure. The HOIG and related integration information may be obtained through the HUD Test Center (HTC).

The HOIG includes HUDware technical information, provides direction to configure and install an application, and identifies steps to take during development to successfully integrate a system and make support and maintenance of that system more efficient in the HUD production environment.

A) WHAT

Comply with all guidelines and technical requirements applicable to your project to successfully integrate your system into the HUD environment.

B) WHY

The HUD Test Center (HTC) will reject any system if it does not comply with HOIG and HUDware technical requirements and your product will not be released into production.

C) WHEN

Early in the lifecycle when considering platform options in the Define System phase and subsequently during the Design System phase as part of the decision making process, and finally in the Build System phase to ensure compliance with the requirements is adhered to as your project is developed.

HUD TEST CENTER (HTC) AND THE SOFTWARE RELEASE PROCESS

Testing by the HUD Test Center (HTC) staff focuses on the non-mainframe platforms. The HTC staff examines the installation procedures and connectivity of an application when integrated into the HUD environment. Release testing does not assess the functionality of the application.

The HTC performs release testing for all HUD Client/Server, LAN, Lotus Notes, and Internet/Intranet applications. All non-mainframe applications must pass release testing prior to production implementation. In addition, the HTC is available to support development and functionality testing with proper notification and scheduling.

All release requests, regardless of platform, must be submitted through the HUD Application Release Tracking System (HARTS). HARTS is a Lotus Notes system used by the HUD development and operations organizations to create and process application releases.

A) WHAT

Schedule the release testing of your application through the HTC. Upon successful completion of the release testing process, the HTC will forward your application to be implemented into production. Coordinate production release with the appropriate OIT, HQ, Regional and/or Field Offices.

B) WHY

Your application will not be released into production without successfully completing HTC release testing.

C) WHEN

During the Evaluate System phase of the SDM lifecycle; once the system successfully completes unit and user-acceptance testing and the development team certifies the system production-ready, release testing is performed.

INVENTORY OF AUTOMATED SYSTEMS (IAS)

The Inventory of Automated Systems (IAS) is a web-based application that maintains key information on HUD systems including system code and acronym, description, technical profile, and points-of-contact. The IAS identifies official financial systems, provides hardware and software information, and has additional details including the CM tool and platform associated with each application.

HUD uses the IAS to manage its inventory of systems, identify critical systems, and understand the implications of platform changes. The IAS allows developers, users and managers access to background information on all active systems.

A) WHAT

Obtain an IAS system code for your new system. Keep the information about existing systems up-to-date; all Project Leaders are responsible for keeping the IAS records for their systems current.

B) WHY

HTC cannot conduct release testing AND a system cannot be released into production without an IAS system code.

C) WHEN

Once funding for the project is approved and you and your development team have made a platform determination, acquire an IAS system code.

Update the IAS when there are changes to the system or platform. In addition, update the IAS when there is any change of support personnel, such as key points of contact.

SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act of 1973 gives all people with disabilities, whether HUD employees or the public, the right to equal access to all electronic and information technology of any Federal agency.

Section 508 Accessibility Standards apply to information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion or duplication of data or information.

A) WHAT

Verify that any new application, major modification, hardware purchase, or software purchase complies with applicable Section 508 Accessibility Standards. No new or modified application will be released into production if it is not Section 508-compliant.

B) WHY

Section 508 requires Federal agencies to provide equal access to information technology to employees and members of the public with disabilities.

C) WHEN

Initially, Section 508 considerations must be addressed as part of the IT capital planning and procurement processes.

- ✓ Configuration Change Management Board (CCMB) approval for non-standard products is contingent on compliance with HUD Section 508 policies
- ✓ HUD-approved accessibility technology is included on the **IT Standards** page of **hud.gov**

Applicable Section 508 Accessibility Standards are included in the requirements documentation produced during Define System phase of the SDM lifecycle and, subsequently, are an integral part of the design documentation produced during the Design System phase.

SECURITY

All HUD Offices must ensure their systems provide adequate security measures for the information collected, processed, transmitted, stored, or disseminated from its applications and support systems. The system category (major application, general support system, or non-major application), criticality and sensitivity of system information, along with availability, integrity and confidentiality requirements, together help determine the security measures appropriate for an application.

E-Government initiatives and **FISMA** requirements highlight the importance of security planning. All federal systems have value and should be covered by a security plan. Applications should be covered individually if they are designated as major applications, or within the security plan of a general support system. **OMB Circular A-130** prescribes specific activities to support compliance with the Computer Security Act, Privacy Act, and related legislation.

A) WHAT

Develop and maintain a **System Security Plan** in accordance with **SDM** requirements, HUD **Information Security** policies, current **NIST** guidance, and the requirements of **OMB Circular A-130, Appendix III**.

B) WHY

The law mandates adequate security safeguards are in place to protect HUD information processing resources and sensitive data. Adhering to these processes protects the integrity of HUD systems and information, and reduces operational risk exposure.

Non-compliance may lead to the compromise of sensitive data, negatively impact HUD operations, and can also result in adverse IG and/or GAO audit findings.

C) WHEN

Initially, develop the **System Security Plan** after requirements have been documented during the Define System phase of the SDM lifecycle; subsequently, update the plan when any enhancements or major modifications are made to the system.

Review the plan at least once every three (3) years and update as warranted.

MAJOR APPLICATIONS

OMB Circular A-130, Appendix III requires that a **System Security Plan** be developed and maintained for all systems designated as major applications or general support systems. The **NIST (SP) 800-18** and **(SP) 800-64** provide additional specifics concerning application security planning requirements. To develop an appropriate security plan for your project, it is necessary to determine whether it is a major application or general support system.

A major application typically has the characteristics noted below. These can be determined by review of a system profile, needs statement, or similar documents:

- Performs clearly defined functions for which there are readily identifiable security considerations and needs.
- Special management oversight of security is required due to the criticality of the application to the HUD mission, or due to the sensitivity of information contained in, processed, transmitted or stored by the application.
- The potential impact should there be a security breach is moderate to high as defined by the **FIPS 199** security categorization. Protection requirements for confidentiality, integrity and availability range from medium to high.

A) WHAT

Know the key characteristics of major applications and general support systems, and be able to determine which category applies to your project.

B) WHY

There are different security planning requirements and coordination issues applicable to each system category.

C) WHEN

Make the category determination early in the development lifecycle, prior to or in conjunction with developing the **System Security Plan**.

GENERAL SUPPORT SYSTEMS

OMB Circular A-130, Appendix III requires that a **System Security Plan** be developed and maintained for all systems designated as general support systems or major applications. The **NIST (SP) 800-18** and **(SP) 800-64** provide additional specifics concerning security planning requirements. In order to develop an appropriate security plan for your project, you must determine whether it is a general support system or a major application.

A general support system typically can be identified by the characteristics noted below. These can be determined by review of a system profile, needs statement, or similar documentation:

- The system is part of the agency infrastructure or provides infrastructure support. Examples include an agency wide backbone, LAN, or communications network.
- The system provides support for a variety of users, and/or supports or hosts a variety of applications.
- The potential impact of a security breach could be low, medium or high as defined by the **FIPS 199** security categorization

A) WHAT

Know the key characteristics of major applications and general support systems, and be able to determine which category applies to your project.

B) WHY

There are different security planning requirement and coordination issues applicable to each system category.

C) WHEN

Make the category determination early in the development lifecycle, prior to or in conjunction with developing the **System Security Plan**.

A-130 REVIEWS

Appendix III of OMB Circular A-130 establishes a minimum set of controls to be included in Federal automated information security programs. The A-130 Review is an evaluation of these security controls for major applications and general support systems.

The A-130 requires the owner/sponsor of a system to review, and update as needed, the **System Security and Privacy Plan** at least once every three (3) years or as an event (such as a major enhancement or modification) may warrant.

Approximately fifteen to twenty-five (15-25) mission critical and/or financial systems are selected for review each year. A-130 Reviews assess four (4) main control areas:

- ✓ Assignment of responsibility for system security
- ✓ The **System Security and Privacy Plan**
- ✓ Periodic review of application controls
- ✓ Authorization to process

In addition to assessing the main control areas, the A-130 Review examines the following seven (7) secondary control areas that should be addressed by the Security Plan:

- ✓ Establishing rules of behavior
- ✓ Personnel security
- ✓ Security training
- ✓ Contingency planning
- ✓ Information sharing
- ✓ Public access controls
- ✓ Technical controls

A) WHAT

Comply with requirements outlined in **Appendix III of OMB Circular A-130**. When your system is selected for an A-130 Review, provide the review team with access to requested system documents and/or key personnel.

B) WHY

A-130 Reviews are not optional; when a project is selected for review, providing access to system documentation and/or key personnel is mandatory.

C) WHEN

Provide access to the requested system documents and/or key personnel upon request of the Security staff.

SYSTEM DEVELOPMENT METHODOLOGY (SDM)

HUD utilizes a system development lifecycle model called the **System Development Methodology (SDM)**. The **SDM** defines HUD policies and procedures for system development, details the requirements for supporting documentation, and provides the templates and checklists to produce required project documentation.

This methodology is flexible and can accommodate all types of development lifecycles including prototyping, waterfall, incremental, or legacy systems maintenance.

A) WHAT

Follow the SDM for all development projects. Project Leaders are expected to know the **SDM** and use the functions and products to develop quality systems.

B) WHY

All HUD Information Systems development projects must comply with the **SDM**. The **SDM** was developed to facilitate effective management of the Department's IT resources and will help ensure HUD compliance with the Clinger-Cohen Act.

Following the **SDM** will help the Project Leader successfully manage a project in order to deliver a quality product that meets user requirements, is on time and within budget.

C) WHEN

Initially, at project inception, review the **SDM**. Utilize the SDM products list and procedures as the basis for the deliverables listed in the Project Plan.

IT CAPITAL PLANNING AND INVESTMENT MANAGEMENT

IT Capital Planning and Investment Management is comprised of multiple HUD initiatives geared towards improving the overall IT investment, acquisition, and management processes at HUD. The following elements are key components of the HUD IT Capital Planning and Investment Management effort:

- ENTERPRISE ARCHITECTURE (EA)
- IT CAPITAL PLANNING
- SOFTWARE ACQUISITION INITIATIVE (SA-CMM)

ENTERPRISE ARCHITECTURE

A current HUD objective is to realize more effective IT Capital Planning and investment. **Enterprise Architecture (EA)** is a Department-wide initiative to align Information Technology (IT) with this core objective.

Enterprise Architecture (EA) is a proactive effort that involves Program Office and IT staff in identifying strategic objectives, associated business and information technology needs, and facilitates the development of re-aligned IT solutions to deliver improved quality service. EA blueprints have been developed that define the data, applications and platforms that support the Department's core services, and can be shared by multiple information systems.

A) WHAT

Review the **EA Policy** and **EA Information Technology Blueprints** at HUD and understand the characteristics and layers of the EA model.

B) WHY

Adherence to the **Enterprise Architecture (EA)** initiative at HUD supports compliance with the Clinger-Cohen Act and related OMB requirements.

C) WHEN

Consider the **EA** when planning any new development or major enhancement projects.

IT CAPITAL PLANNING

IT Capital Planning is a systematic approach to managing the risks and returns of HUD IT investments. IT investment management features three distinct processes crucial to maximizing the performance of the HUD IT investment portfolio:

- Select
- Control
- Evaluate

A) WHAT

All HUD IT projects must comply with capital planning guidelines and reporting requirements. Become familiar with the HUD IT Investment Management process, provide timely information in response to all data calls, and follow the published procedures for all capital planning and investment management activities.

B) WHY

Continued funding for your system/project may be jeopardized if you do not follow the required procedures. The HUD IT Investment Management process directly supports compliance with the Clinger-Cohen Act and related OMB requirements.

C) WHEN

Keep the HUD project document repositories up to date on an ongoing basis. Some IT capital planning activities are performed monthly; others are required on a quarterly basis, and there are additional annual capital planning requirements.

Comply with all periodic data calls, including those associated with the Select process, as well as Control reviews.

SOFTWARE ACQUISITION CAPABILITY-MATURITY MODEL INITIATIVE

The Software Acquisition Capability-Maturity Model (SA-CMM) is a set of key process areas applicable to the acquisition of all types of software. The SA-CMM defines five (5) levels of process maturity (Level 1-Level 5); each ascending maturity level is comprised of related common features and key process areas, which lead to a more consistent and disciplined software acquisition process.

The goal of the Software Acquisition Capability-Maturity Model (SA-CMM) initiative at HUD is to apply sound, proven software acquisition principles, as well as continuous process improvement, to the software acquisition process. Detailed information about HUD SA-CMM policy requirements can be found in **HUD Handbook 3262.1, Software Acquisition Capability - Maturity Model Policy**.

A) WHAT

Become familiar with the SA-CMM Initiative. Review the **HUD SA-CMM Policy Handbook** and incorporate these processes into your project planning.

B) WHY

Repeatable project management processes will be established to plan all aspects of software acquisition, manage requirements, track project performance, manage a project's cost and schedule baselines, evaluate project deliverables, and successfully transition the software to its support organization.

C) WHEN

This process is followed in every phase of project development throughout the project lifecycle.

CONTINGENCY PLANNING

Information Technology systems are vulnerable to a variety of disruptions from different sources. These vulnerabilities range from mild (server or network failure) to severe (facility destruction) and can be the result of natural disasters or acts of terrorism. While most vulnerability can be minimized or eliminated through technical or operational solutions, it is impossible to eliminate all risks.

Contingency Planning is a management policy of predetermined and documented procedures designed to maintain or restore business/program operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. While contingency planning is typically associated with the operations and maintenance stages of the system lifecycle, appropriate contingency measures should be identified and integrated during all lifecycle phases.

Effective, tested, and documented contingency plans are crucial to the resumption of essential agency functions. Procedures and capabilities needed for recovering key systems and restoring program operations are documented within the Continuity of Operations Plan, the Business Resumption Plan, and the Disaster Recovery Plan.

Although all of the plans document the procedures for recovery from operational disruptions at HUD, each plan varies based on the severity of the disruption:

- **CONTINUITY OF OPERATIONS PLAN (COOP)**

  A Continuity of Operations Plan (COOP) is a predetermined and documented set of instructions or procedures that describe how HUD Offices will sustain essential functions as a result of a disaster event before the return to normal operations. HUD requires a plan for sustainability of up to 30 days.

  The COOP focuses on the short-term restoration of essential agency functions and the performance of these functions at an alternate site.

- **BUSINESS RESUMPTION PLAN (BRP)** **<SECTION TO BE ADDED>**

  A Business Resumption Plan (BRP) is a documented set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred.

  The BRP addresses the restoration of business processes after an emergency, but unlike the COOP, typically does not include the specific, short-term procedures for the continuity of critical processes through an emergency or disruption.

- **DISASTER RECOVERY PLAN (DRP)** **<SECTION TO BE ADDED>**

  A Disaster Recovery Plan (DRP) is a predetermined and documented set of instructions for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

  The DRP documents recovery procedures from more catastrophic events that can deny facility access for an extended period. The DRP is designed to restore system or facility operability at an alternate site after an emergency; the DRP is narrow in scope and typically does not address minor disruptions that do not require relocation.

CONTINUITY OF OPERATIONS PLAN (COOP)

All HUD Offices must have viable COOP plans and procedures to ensure the continuity of essential functions during emergencies or other situations that may disrupt normal operations. The Emergency Planning and Management Division of the **Office of Security and Emergency Planning** has the lead role in agency-wide COOP development and planning. The Chief Technology Officer (CTO) coordinates the development of COOP IT plans and manages the disaster recovery plans for HUD IT systems.

HUD requirements for COOP planning are detailed in the HUD COOP Handbook 3205.1. The provisions of the HUD COOP Handbook 3205.1 apply to all principal organizations in HUD headquarters, as well as Regional and Field Offices.

There is a detailed COOP plan for each HUD operating platform or environment (Notes, Unisys, &c.). While IT Operations plays a key role upon COOP plan activation, there are steps the Project Leader can take to assist in this scenario if called upon.

A) WHAT

Know your system and be aware of its role in support of essential agency functions. Respond quickly to any requests for information or assistance pertaining to COOP plan development, testing, or implementation.

B) WHY

Maintaining essential HUD functions during emergencies or other disruptions are part of the agency mission as a responsible public institution.

C) WHEN

The Project Leader must be able to provide any requested information to aid in the creation and maintenance of the COOP at any given time.

HUD IT ENVIRONMENT

In order to plan and manage an IT project at HUD, knowledge of a few basic support functions outside of the system development process itself is essential.

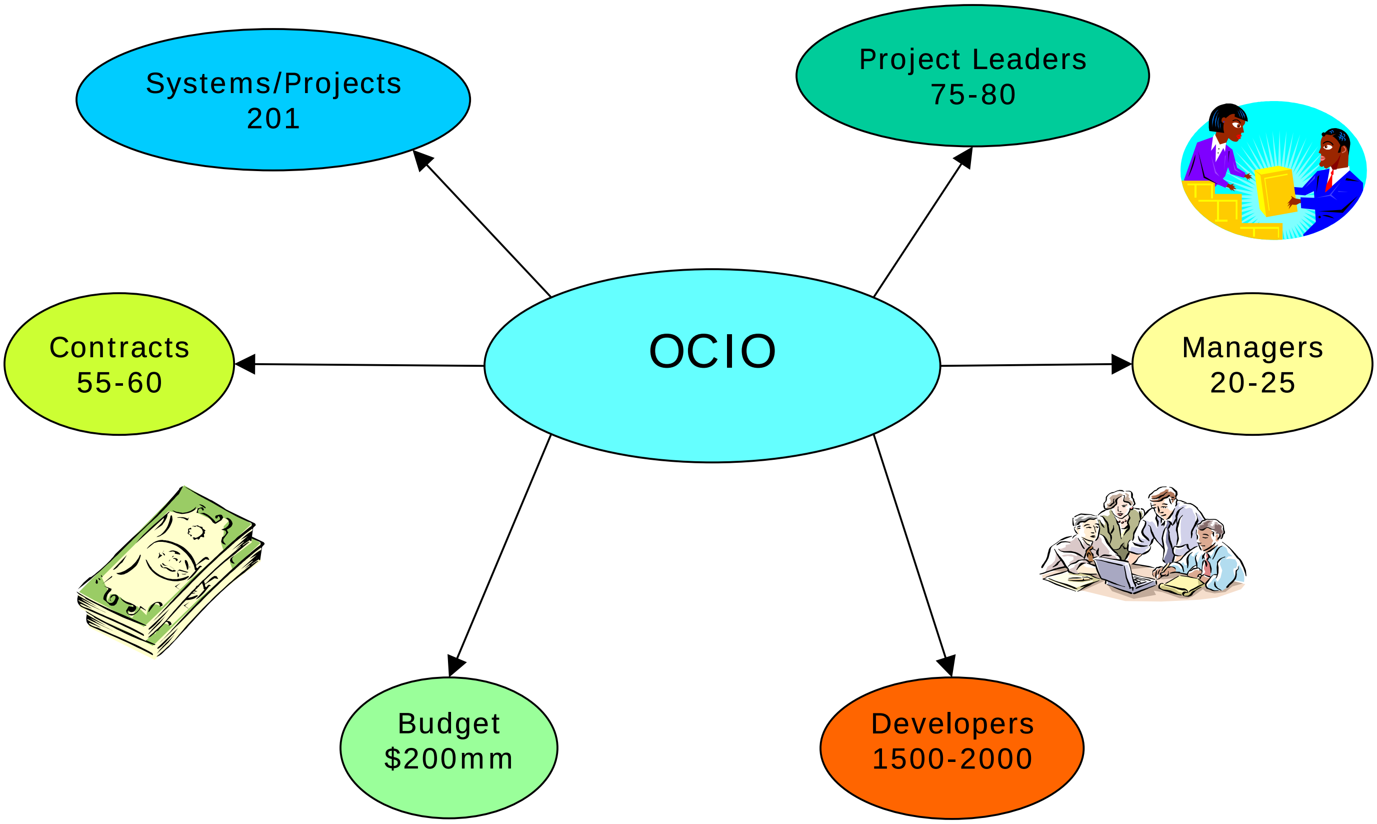
- **CONTRACTING**
- **OFFSITE CONTRACTOR CONNECTIVITY**
- **IT HELP AT HUD**

Successful IT projects are collaborative efforts; HUD IT and Program Office staff must work together with contractors, vendors and other business partners to achieve Departmental goals through the use of information technology.

Some characteristics of the HUD IT environment include:

1) Over 200 Projects
2) Over 75 Project Leaders
3) Over 55 contracts with an annual budget exceeding $200 million
4) Approximately 200 applications and support systems

System Development at HUD



CONTRACTING

HUD utilizes the services of contractors for most system development projects. The Project Leader will work with both contractor and HUD staff during the lifecycle of a typical system or project. Therefore, some basic knowledge of the contracting process is essential.

Contracting at HUD falls within the purview of the **Office of the Chief Procurement Officer (OCPO)**. Key elements of the contracting process are the procurement of contract services, as well as management and oversight of the contract once it is in place.

All HUD polices concerning contracting and procurement are based on the **Federal Acquisition Regulation (FAR)** and the **HUD Acquisition Regulation (HUDAR)**.

The preferred approach to contracting at HUD today involves the use of fixed price, performance-based contracts where contractor payment is tied to the achievement of specific goals and objectives detailed in the contract and Statement of Work (SOW). The SOW is a crucial document that spells out the work to be performed under the contract and references specific work products and deliverables.

The SOW must address any government facilities or equipment to be furnished or acquired during the task. HUD does not typically provide facilities, computers or other systems for contractor use any longer; however, if HUD connectivity for offsite contract staff is required, follow current procedures and coordinate with your GTM/GTR and OIT staff.

HUD Contracting Staff is available to support the contracting needs of all principal HQ and Field Office organizations.

A) WHAT

Understand the basics of contracting at HUD including how to write a clear, valid SOW. Know what is required to properly manage and oversee the contractor's work once the contract is awarded.

B) WHY

HUD relies on contractors for most system development efforts. Not understanding the basics of contracting can lead to delays in any procurement actions for your project, as well as problems with contractor performance.

C) WHEN

A Project Leader may have to procure and manage contract services at any time; understanding the basics is an on-going process.

OFFSITE CONTRACTOR CONNECTIVITY

System development at HUD today is typically performed by contractors, many of which are located at remote locations. HUD normally does not provide facilities, computers or other equipment for its contractors.

HUD will provide network connectivity to offsite contractors that are approved for remote access and comply with a specific set of security and technical requirements. Offsite connectivity options include Virtual Private Network (VPN) software, point-to-point circuits, and dial-up access.

The basic requirements for remote contractor access are:

- The contractor must have a current contract with HUD to develop, maintain, and/or support HUD applications.
- The contractor must have GTM/GTR contractual approval for remote access.
- Office of Information Technology (OIT) management review (and approval) for adherence to security and technical requirements, policies and procedures.

A) WHAT

Work with your GTM/GTR, OCPO, and contractor staff to ensure that contractual obligations regarding connectivity are followed. Know the basic policies and procedures for offsite contractor connectivity.

B) WHY

Your project schedule may be negatively impacted if offsite connectivity issues and requirements are not properly understood and addressed. Connectivity will not be provided for your contractors until all issues are resolved and offsite access is approved.

C) WHEN

Offsite connectivity requirements should be considered when developing requests for proposals, statements of work, evaluating proposals, and at contract implementation.

IT HELP AT HUD

The Customer Service Division (CSD) of the Computer Services, Operations and Maintenance Group (CSOMG) plays the lead role in providing IT user help and support to HUD and contract staff at HQ. Field Office staff is supported by the Information Technology Division of their respective Administrative Service Center (ASC).

CSD works to resolve a wide variety of problems, including hardware, software, and network related issues. The Service Ticket Action Resolution System (STARS) is the primary HUD tool used for IT problem tracking and reporting.

If you have an IT problem, contact the Help Desk for assistance.

For some basic problems such as password re-sets, the Help Desk typically can work with you to resolve the issue while you are on the telephone; in other instances the problem may be assigned to the appropriate support group for resolution. In these situations, a STARS ticket number will be issued to you.

It is important you write down the STARS ticket number, as this is how the problem you reported is identified and tracked.

A) WHAT

If you encounter IT problems that require assistance, contact the Help Desk at (202) 708-3300 or 1-888-297-8689 and follow the instructions.

B) WHY

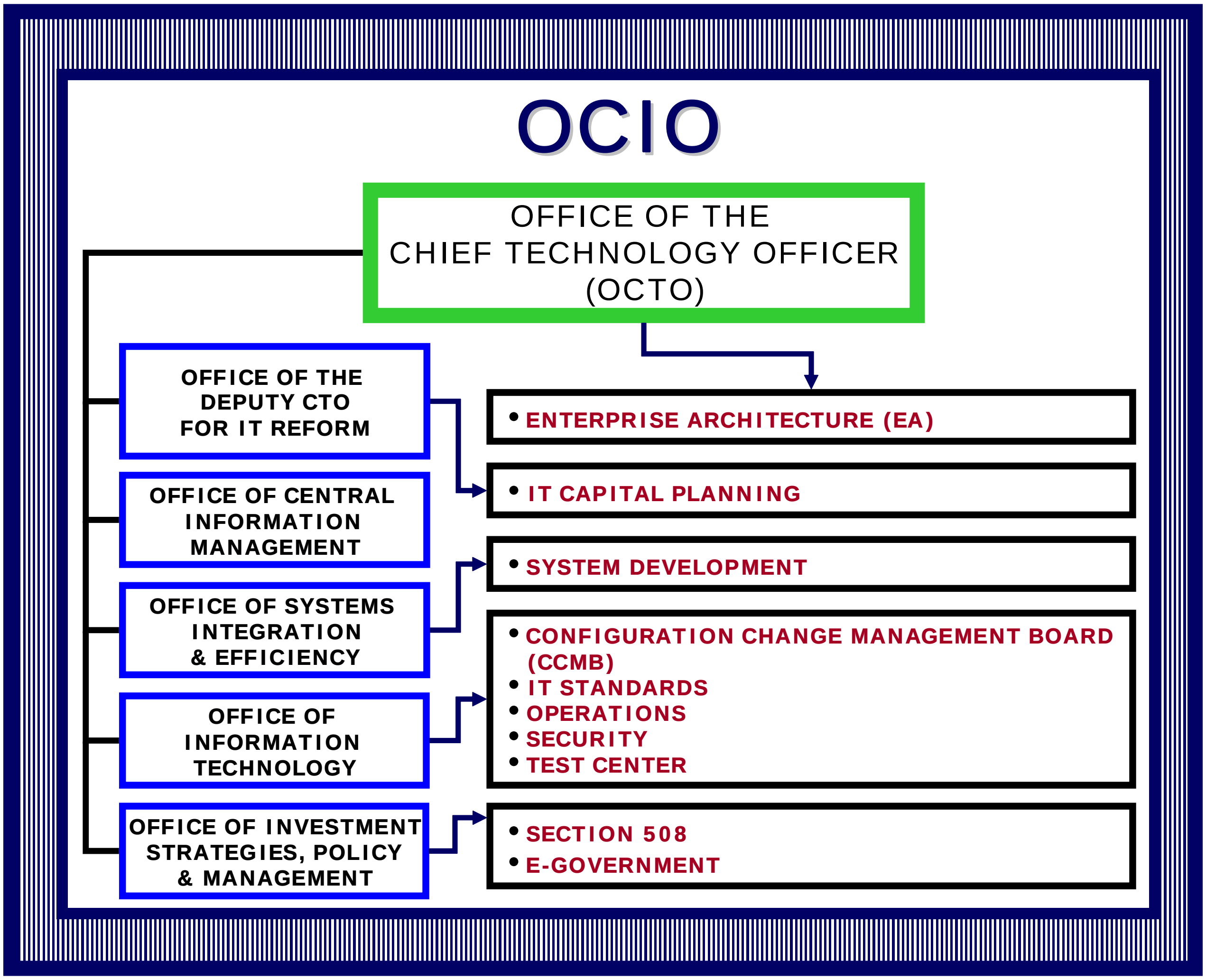
The Help Desk provides the HUD community with a single point of contact for all supported products and services, and is dedicated to the prompt resolution of all IT problems.

C) WHEN

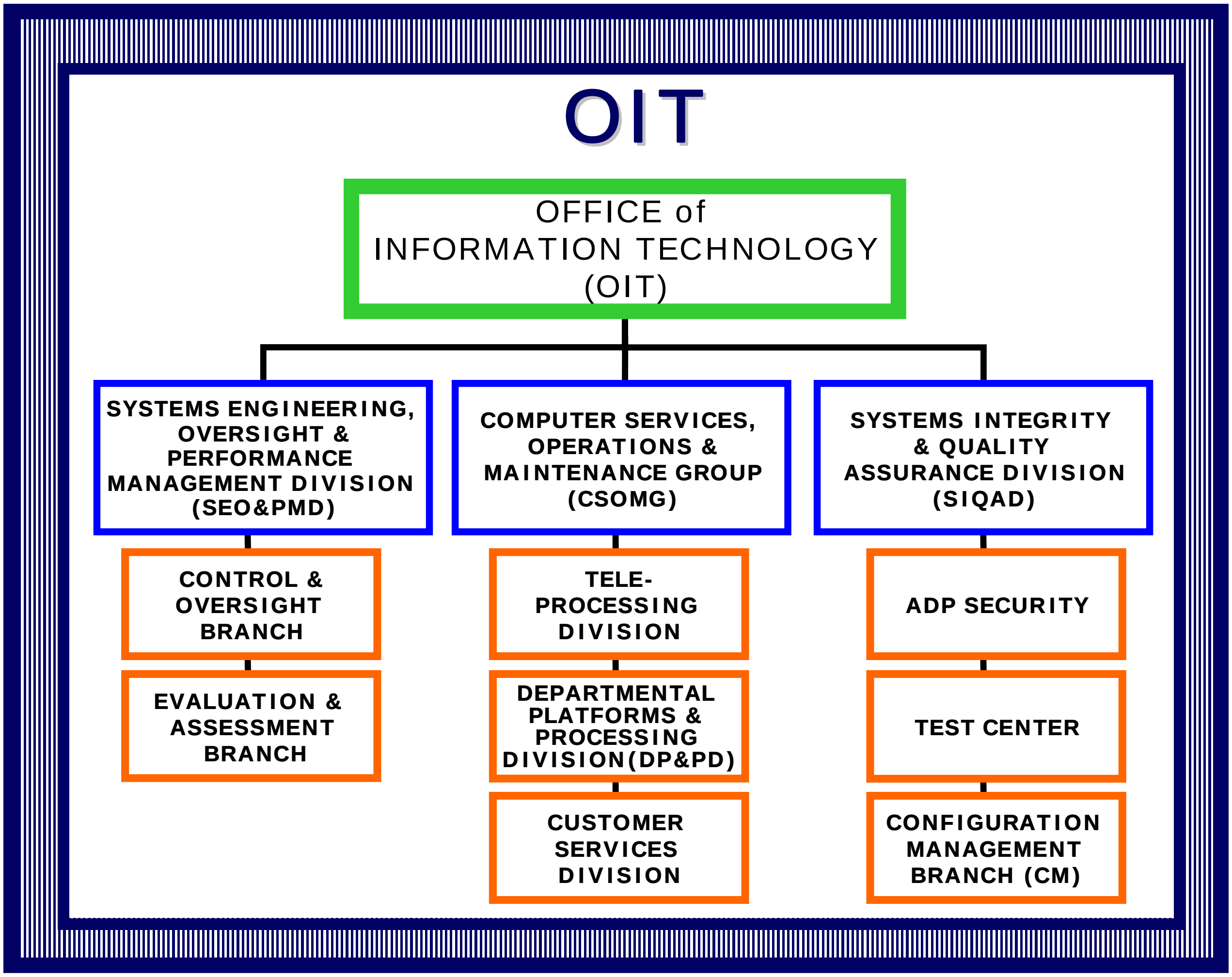
Anytime you require technical assistance between 7:00 a.m. and 8:00 p.m.

APPENDIX A OIT ORGANIZATION AND ROLES

OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)


OCIO
OFFICE OF THE CHIEF TECHNOLOGY OFFICER (OCTO)
OFFICE OF THE DEPUTY CTO FOR IT REFORM
OFFICE OF CENTRAL INFORMATION MANAGEMENT
OFFICE OF SYSTEMS INTEGRATION & EFFICIENCY
OFFICE OF INFORMATION TECHNOLOGY
OFFICE OF INVESTMENT STRATEGIES, POLICY & MANAGEMENT
• ENTERPRISE ARCHITECTURE (EA)
• IT CAPITAL PLANNING
• SYSTEM DEVELOPMENT
• CONFIGURATION CHANGE MANAGEMENT BOARD (CCMB)
• IT STANDARDS
• OPERATIONS
• SECURITY
• TEST CENTER
• SECTION 508
• E-GOVERNMENT

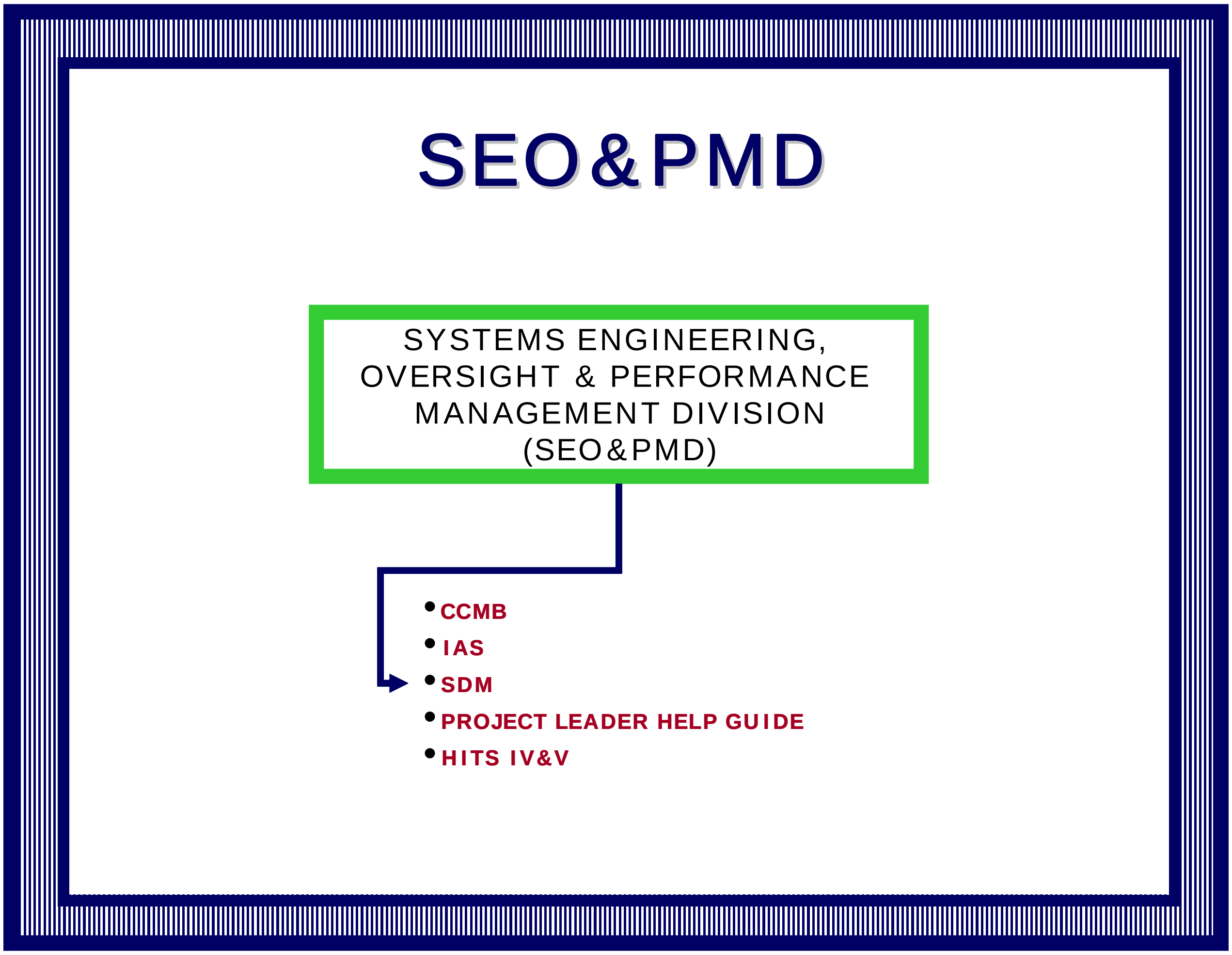
OFFICE OF INFORMATION TECHNOLOGY (OIT)


OIT
OFFICE of INFORMATION TECHNOLOGY (OIT)
SYSTEMS ENGINEERING, OVERSIGHT & PERFORMANCE MANAGEMENT DIVISION (SEO&PMD)
COMPUTER SERVICES, OPERATIONS & MAINTENANCE GROUP (CSOMG)
SYSTEMS INTEGRITY & QUALITY ASSURANCE DIVISION (SIQAD)
CONTROL & OVERSIGHT BRANCH
EVALUATION & ASSESSMENT BRANCH
TELE-PROCESSING DIVISION
DEPARTMENTAL PLATFORMS & PROCESSING DIVISION(DP&PD)
CUSTOMER SERVICES DIVISION
ADP SECURITY
TEST CENTER
CONFIGURATION MANAGEMENT BRANCH (CM)

SYSTEMS ENGINEERING OVERSIGHT AND PERFORMANCE MANAGEMENT DIVISION (SEO&PMD)

RESPONSIBILITIES

- ✓ Publish and maintain IT standards
- ✓ IT Project Management Oversight and Support
- ✓ Coordinate the CCMB process
- ✓ Manage the IAS application
- ✓ System Development Methodology (SDM)
- ✓ HUD Information Technology Services Independent Verification and Validation (HITS IV&V)



SEO&PMD

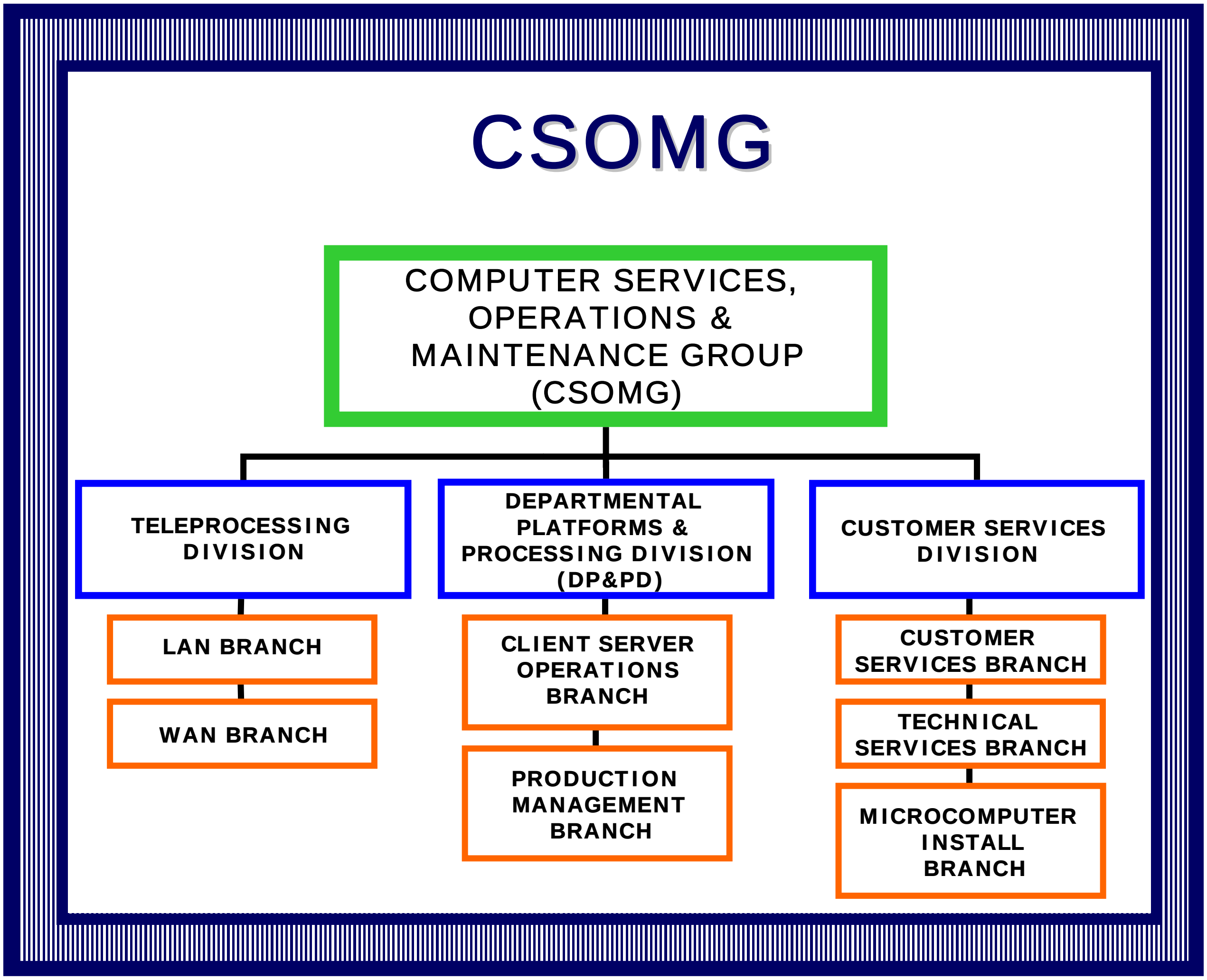
SYSTEMS ENGINEERING, OVERSIGHT & PERFORMANCE MANAGEMENT DIVISION (SEO&PMD)

- CCMB
- IAS
- SDM
- PROJECT LEADER HELP GUIDE
- HITS IV&V

COMPUTER SERVICES, OPERATIONS & MAINTENANCE GROUP (CSOMG)

RESPONSIBILITIES

- ✓ LAN, WAN, and Internet/Intranet infrastructure and support
- ✓ Client/server and Mainframe operations
- ✓ Data Center and Development & Recovery facility management
- ✓ User support and help desk services


CSOMG

COMPUTER SERVICES, OPERATIONS & MAINTENANCE GROUP (CSOMG)

TELEPROCESSING DIVISION

LAN BRANCH

WAN BRANCH

DEPARTMENTAL PLATFORMS & PROCESSING DIVISION (DP&PD)

CLIENT SERVER OPERATIONS BRANCH

PRODUCTION MANAGEMENT BRANCH

CUSTOMER SERVICES DIVISION

CUSTOMER SERVICES BRANCH

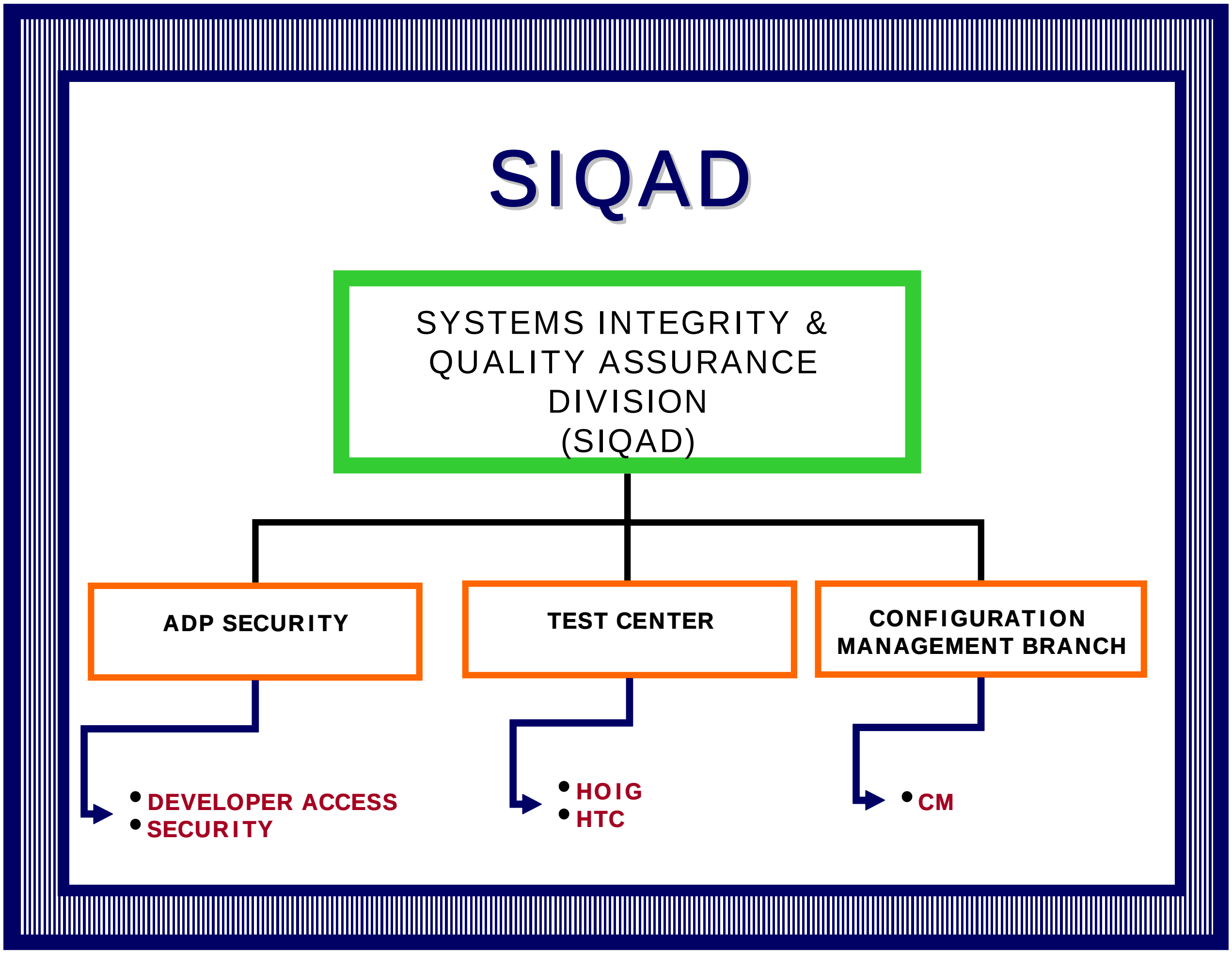
TECHNICAL SERVICES BRANCH

MICROCOMPUTER INSTALL BRANCH

SYSTEMS INTEGRITY AND QUALITY ASSURANCE DIVISION (SIQAD)

RESPONSIBILITIES

- ✓ ADP Security management and support
- ✓ Infrastructure protection
- ✓ A-130 Reviews
- ✓ Configuration Management
- ✓ HUD Test Center management
- ✓ Application release support


SIQAD
SYSTEMS INTEGRITY & QUALITY ASSURANCE DIVISION (SIQAD)
ADP SECURITY
TEST CENTER
CONFIGURATION MANAGEMENT BRANCH
• DEVELOPER ACCESS
• SECURITY
• HOIG
• HTC
• CM

APPENDIX B ACRONYMS

BRP	Business Resumption Plan
CCMB	Configuration Change Management Board
CM	Configuration Management
CMP	Configuration Management Plan
COOP	Continuity of Operations Plan
COTS	Commercial-Off-the-Shelf
CSOMG	Computer Services, Operations & Maintenance Group
DCB	Data Control Board
DP&PD	Departmental Platforms & Processing Division
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
ECPIC	Electronic Capital Planning And Investment Control
EIT	Electronic and Information Technology
EDM	Enterprise Data Management
FFAS 10	Federal Financial Accounting Standard 10
GPEA	Government Paperwork Elimination Act
GTM	Government Technical Monitor
GTR	Government Technical Representative
HARTS	HUD Application Release Tracking System
HITS	HUD Information Technology Services
HOIG	HUD Open Integration Guidelines
HTC	HUD Test Center
IAS	Inventory of Automated Systems
IG	Inspector General
IT	Information Technology
IV&V	Independent Verification & Validation
LAN	Local Area Network
OAMS	Office of Administrative and Management Services
OCFO	Office of the Chief Financial Officer
OCIO	Office of The Chief Information Officer
OIT	Office of Information Technology
OMB	Office of Management and Budget
PMR	Project Management Review
SA-CMM	Software Acquisition Capability Maturity Model
SDM	System Development Methodology
SEOPMD	Systems Engineering, Oversight & Performance Management Division
SIQAD	Systems Integrity & Quality Assurance Division
TIBEC	Technology Investment Board Executive Committee
VPN	Virtual Private Network
WCF	Working Capital Fund

APPENDIX C GLOSSARY

AVAILABILITY

AVAILABILITY

Availability is the assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely basis and are protected from denial of service. Availability requirements are part of realistically determining the criticality/sensitivity of system information.

BUSINESS RESUMPTION PLAN (BRP)

BUSINESS RESUMPTION PLAN (BRP)

A Business Resumption Plan (BRP) is a documented set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred.

CONFIDENTIALITY

CONFIDENTIALITY

Confidentiality is the assurance that information in an IT system is not disclosed to unauthorized persons, processes or devices. Confidentiality requirements are part of accurately assessing the criticality/sensitivity of system information.

CONTINGENCY PLANNING

CONTINGENCY PLANNING

Contingency Planning is a management policy of predetermined and documented procedures designed to maintain or restore business/program operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

CONTINUITY OF OPERATIONS PLAN (COOP)

CONTINUITY OF OPERATIONS PLAN (COOP)

A Continuity of Operations Plan (COOP) is a predetermined and documented set of instructions or procedures that describe how HUD Offices will sustain essential functions as a result of a disaster event before the return to normal operations. HUD requires a plan for sustainability of up to 30 days.

CRITICALITY/SENSITIVITY

CRITICALITY/SENSITIVITY

Criticality/Sensitivity refers to the importance and nature of information processed, stored, and transmitted by an IT system to HUD's mission and day-to-day operations. Requirements for availability, integrity, and confidentiality must be considered when assessing the criticality/sensitivity level of system information, and can help determine the appropriate safeguards to be incorporated into the System Security Plan.

DATA CALLS

DATA CALLS

Data calls are periodic requests for project information issued by the Office of IT Reform and support the HUD IT Investment Management process to ensure HUD IT projects perform within acceptable parameters.

Data call specifics may vary, but typically require updated project cost, schedule, and technical performance information to be entered in I-TIPS and/or Project Office. These requests may be in conjunction with quarterly Control Reviews or the annual Select Process.

DATA QUALITY

DATA QUALITY

Data Quality is the assurance of the accuracy and integrity of data input to HUD applications, data processed by HUD applications, or data output from HUD applications. Incorporating controls such as pick lists, data entry edits, or filters into your application design can enhance data quality.

DISASTER RECOVERY PLAN (DRP)

DISASTER RECOVERY PLAN (DRP)

A Disaster Recovery Plan (DRP) is a predetermined and documented set of instructions for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

E-GOVERNMENT

E-GOVERNMENT

E-Government provides on-line access to government information and services. The initiatives of E-Government include web-based technologies designed around the needs of the public and/or HUD business partners that enable HUD to automate paper-based functions and services. E-Government reduces the amount of paper processed by HUD staff and supports HUD compliance with the **Government Paperwork Elimination Act (GPEA)**.

FFAS 10

FEDERAL FINANCIAL ACCOUNTING STANDARD NUMBER 10

FFAS 10 establishes accounting standards for the costs of internal use software; guidance is provided regarding the types of costs to capitalize, capitalization timing and thresholds, amortization periods, and other related accounting rules within the wording of the rule.

FFAS 10 requires capitalization of the costs (costs cannot be expensed) of internal use software. FFAS 10 rules apply to all HUD IT projects with lifecycle acquisition and development costs of $1 million or more and applies regardless of whether the software is contractor-developed, internally developed or a COTS (Commercial-Off-the-Shelf) package.

FINANCIAL SYSTEM

FINANCIAL SYSTEM

A financial system is an information system comprised of one or more applications that is used for collecting, processing maintaining, transmitting, and reporting data about financial events; supporting financial planning or budgeting activities; accumulating and reporting cost information; or supporting the preparation of financial statements.

Some HUD systems are designated as *official financial systems* by the OCFO (Office of the Chief Financial Officer), and therefore require additional project management and operational controls, as well as supporting documentation.

GENERAL SUPPORT SYSTEM

GENERAL SUPPORT SYSTEM

A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications and people, and provides support for a variety of users and/or applications. A general support system can be, for example, a local area network (LAN) that supports a branch office, an agency-wide backbone, communications network, a departmental data processing center including its operating system and utilities, or a shared information processing service organization (ISPO).

GTM

GOVERNMENT TECHNICAL MONITOR

The GTM helps with practical issues such as coordinating building and computer access for contract staff and obtaining government-furnished property required by the contractor. The GTM assists the GTR, and may be delegated many of the duties of a GTR.

GTR

GOVERNMENT TECHNICAL REPRESENTATIVE

The GTR provides contractors technical advice and guidance related to work required by the contract. The GTR is also the principal judge of a contractor's performance, including the quality and timeliness of work, and the contractor's ability to control costs. The GTR is expected to be knowledgeable in the technical area(s) covered by the contract.

INTEGRITY

INTEGRITY

Integrity is the assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. Integrity requirements are part of realistically determining the criticality/sensitivity of system information.

MAJOR APPLICATION

MAJOR APPLICATION

A major application requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. **Note:** All Federal applications require some level of protection. Certain applications, however, because of the information in them, require special management oversight and attention to security, and should be treated as major.

OMB EXHIBIT 300

OMB EXHIBIT 300

OMB Exhibit 300 is a Capital Asset Plan and Justification; it is required for all major projects. For OMB Exhibit 300 purposes, the OCIO Office of IT Reform identifies HUD major projects.

Major projects are defined as those projects that require special management attention because of their importance to a HUD mission, or have high development, operating or maintenance costs, or play a significant role in the administration of agency programs or resources (i.e., financial systems).

OTC

OFFICE TECHNOLOGY COORDINATOR

A designated HUD staff member who assists Program Office personnel on a variety of issues, which may include obtaining LAN and email access, office space, data security, and computer hardware and software needs. The OTC interfaces with OIT staff as needed to help resolve IT problems.

PMRS

PROJECT MANAGEMENT REVIEWS

PMRs are high-level IT project management reviews conducted by the OCIO Project Management Review Board. The PMR process is presently an executive briefing comprised of 10 slides. Specific guidelines for the information covered by each slide, as well as presentation format, are provided by the OCIO in advance of the project review.

PMRs provide a forum to evaluate IT project management capabilities, identify needed improvements, identify new business needs, and offer management support to ensure project success.

PMRs improve the Department’s ability to manage its IT investments, and support compliance with the Clinger-Cohen Act, Paperwork Reduction Act, and OMB guidelines.

WCF

WORKING CAPITAL FUND

The Working Capital Fund is a revolving fund used to finance a continuing cycle of business-type operations in which expenditures will generate collections, which will then be available without further congressional action. Currently at HUD, the WCF is only used to fund information technology services.

APPENDIX D REFERENCES

Enterprise Architecture
http://www.hud.gov/offices/cio/ea/index.cfm

Information Technology Standards
http://www.hud.gov/offices/cio/sdm/devlife/def/newstand.cfm

National Institute of Standards and Technology
http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

National Institute of Standards and Technology (Publications)
http://www.nist.gov/public_affairs/pubs.htm

Office of Administration
http://www.hud.gov/offices/adm/

Office of the Chief Information Officer
http://www.hud.gov/offices/cio/

Office of the Chief Procurement Officer
http://www.hud.gov/offices/cpo/

Office of Management and Budget
http://www.whitehouse.gov/omb/

Project Leader Help Guide
http://www.hud.gov/offices/cio/sdm/pl_help_guide.pdf

System Development Methodology (SDM)
http://www.hud.gov/offices/cio/sdm/index.cfm